THAT WHICH IS CLAIMED IS:

1. A method of message authentication for an SSL-based protocol connection between a source device and a destination device, the method comprising:

generating a group message authentication code (MAC) based on a plurality of communication packets, each of the communication packets having at least one data record; and

transmitting the plurality of communication packets using the SSL-based protocol connection along with the generated group MAC, wherein ones of the plurality of communication packets do not include an associated packet MAC.

2. The method of Claim 1 further comprising transmitting a record count using the SSL-based protocol connection, the record count indicating a number of data records to be received associated with a next group MAC to be received, the data records associated with the record count corresponding to a next plurality of communication packets to be transmitted and wherein the next group MAC is generated based on the next plurality of communication packets to be transmitted.

3. The method of Claim 2 wherein the record count is transmitted using the SSL-based protocol connection before the next plurality of communication packets and wherein the next group MAC is transmitted after the next plurality of communication packets.

4. The method of Claim 3 wherein the record count is transmitted using the SSL-based protocol connection either with the first plurality of communication packets or at a beginning of the next plurality of communication packets.

5. The method of Claim 4 wherein the record count is transmitted following the generated group MAC without any intervening data records.

6. The method of Claim 5 further comprising:

transmitting a last plurality of communication packets using the SSL-based protocol connection along with a last group MAC, the last group MAC being generated based on the last plurality of communication packets; and

closing the SSL-based protocol connection following transmission of the last plurality of communication packets.

7. The method of Claim 5 wherein at least a subset of communication packets from the plurality of communication packets has pre-encrypted data records and wherein the method further comprises:

encrypting data records of the at least a subset of communication packets to provide the pre-encrypted data records;

storing the pre-encrypted data records;

retrieving ones of the stored pre-encrypted data records for transmission responsive to a request for transmission of the ones of the stored pre-encrypted data records;

transmitting the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection without using the SSL-based protocol connection to encrypt the retrieved ones of the stored pre-encrypted data records; and

transmitting a group MAC generated based on the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection to encrypt the group MAC generated based on the retrieved ones of the stored pre-encrypted data records.

8. The method of Claim 7 further comprising establishing the SSL-based protocol connection with a designated client and wherein the pre-encrypted data records are associated with the designated client and wherein the encrypting

step comprises encrypting data records of the at least a subset of communication packets using a public key of the designated client.

9. The method of Claim 8 wherein establishing the SSL-based protocol connection further comprises negotiating a client certificate of the designated client and wherein the method further comprises determining the public key of the designated client based on the client certificate.

10. The method of Claim 7 further comprising establishing the SSL-based protocol connection with a designated client and wherein the pre-encrypted data records are associated with the designated client and wherein the encrypting step comprises encrypting data records of the at least a subset of communication packets using a temporary key known by the designated client.

11. The method of Claim 7 further comprising:

establishing the SSL-based protocol connection with a designated client;

transmitting a pre-encryption key to the designated client using the SSL-based protocol connection; and

wherein the pre-encrypted data records are associated with the designated client and wherein the encrypting step comprises encrypting data records of the at least a subset of communication packets using the pre-encryption key.

12. The method of Claim 11 wherein transmitting a pre-encryption key comprises transmitting the pre-encryption key to the designated client with the record count.

13. The method of Claim 11 further comprising transmitting a plurality of groups of communication packets having pre-encrypted data records, each of the groups of communication packets having an associated group MAC and an associated record count, using the SSL-based protocol connection, wherein the associated group MACs and associated record counts are transmitted using the

SSL-based protocol connection to encrypt the associated group MACs and associated record counts and the pre-encrypted data records are transmitted without using the SSL-based protocol connection to encrypt the pre-encrypted data records, and wherein transmitting a pre-encryption key to the designated client comprises transmitting a pre-encryption key with each of the associated record counts.

14. The method of Claim 5 further comprising the following executed by the destination device.

receiving the first plurality of communication packets and the generated group MAC;

generating a calculated MAC based on the received first plurality of communication packets; and

determining if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received generated group MAC.

15. The method of Claim 14 further comprising terminating the SSL-based protocol connection if it is determined that an error has occurred.

16. The method of Claim 14 further comprising the following executed by the destination device:

receiving the record count;

receiving a number of data records of the next plurality of communication packets corresponding to the received record count;

receiving the next group MAC;

generating a next calculated MAC based on the received data records of the next plurality of communication packets; and

determining if an error has occurred in the received data records of the next plurality of communication packets based on a comparison of the next calculated MAC and the received next group MAC.

17. The method of Claim 1 wherein at least a subset of communication packets from the plurality of communication packets have pre-encrypted data records and wherein the method further comprises:

encrypting data records of the at least a subset of communication packets to provide the pre-encrypted data records;

storing the pre-encrypted data records;

retrieving ones of the stored pre-encrypted data records for transmission responsive to a request for transmission of the ones of the stored pre-encrypted data records;

transmitting the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection without using the SSL-based protocol connection to encrypt the retrieved ones of the stored pre-encrypted data records; and

transmitting a group MAC generated based on the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection to encrypt the group MAC generated based on the retrieved ones of the stored pre-encrypted data records.

18. The method of Claim 17 further comprising establishing the SSL-based protocol connection with a designated client and wherein the pre-encrypted data records are associated with the designated client and wherein the encrypting step comprises encrypting data records of the at least a subset of communication packets using a public key of the designated client.

19. The method of Claim 17 further comprising establishing the SSL-based protocol connection with a designated client and wherein the pre-encrypted data records are associated with the designated client and wherein the encrypting step comprises encrypting data records of the at least a subset of communication packets using a temporary key known by the designated client.

20. The method of Claim 1 further comprising the following executed by the destination device:

receiving the first plurality of communication packets and the generated group MAC;

generating a calculated MAC based on the received first plurality of communication packets; and

determining if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received generated group MAC.

21. The method of Claim 20 further comprising terminating the SSL-based protocol connection if it is determined that an error has occurred.

22. A method for message authentication for an SSL-based protocol connection between a source device and a destination device, the method comprising:

receiving a first plurality of communication packets and a group MAC that was generated based on the first plurality of communication packets, wherein ones of the first plurality of communication packets do not include an associated packet MAC;

generating a calculated MAC based on the received first plurality of communication packets; and

determining if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received group MAC.

23. The method of Claim 22 further comprising:

receiving a record count, the record count indicating a number of data records to be received before a next group MAC, the next group MAC being generated based on a next plurality of communication packets corresponding the data records associated with the record count;

receiving a number of data records of the next plurality of communication packets corresponding to the received record count;

receiving the next group MAC;

generating a next calculated MAC based on the received data records of the next plurality of communication packets; and

determining if an error has occurred in the received data records of the next plurality of communication packets based on a comparison of the next calculated MAC and the received next group MAC.

24. The method of Claim 23 wherein the record count is received using the SSL-based protocol connection before the data records of the next plurality of communication packets corresponding to the received record count.

25. The method of Claim 24 wherein the record count is received after the first group MAC without any intervening data records.

26. A system of message authentication for an SSL-based protocol connection between a source device and a destination device, the system comprising:

a group message authentication code (MAC) generation circuit that generates a group MAC based on a plurality of communication packets, each of the communication packets having at least one data record; and

a transmitter that transmits the plurality of communication packets using the SSL-based protocol connection along with the generated group MAC, wherein ones of the plurality of communication packets do not include an associated packet MAC.

27. The system of Claim 26 further comprising:

a record count generation circuit that generates a record count indicating a number of data records to be received associated with a next group MAC to be received, the data records associated with the record count corresponding to a next plurality of communication packets to be transmitted;

wherein the transmitter is further configured to transmit the record count using the SSL-based protocol connection; and

wherein the group MAC generation circuit is further configured to generate the next group MAC based on the next plurality of communication packets to be transmitted.

28. The system of Claim 27 further comprising an SSL-based connection control circuit that closes the SSL-based protocol connection following transmission of a last plurality of communication packets.

29. The system of Claim 27 further comprising:

a pre-encryption circuit that encrypts data records of at least a subset of communication packets of the plurality of communication packets based on either a temporary key or a client key associated with a designated client associated with the SSL-based protocol connection to provide pre-encrypted data records; and

wherein the transmitter is further configured to transmit the pre-encrypted data records without using the SSL-based protocol connection to encrypt the pre-encrypted records and to transmit a group MAC generated based on the pre-encrypted data records using the SSL-based protocol connection to encrypt the group MAC generated based on the pre-encrypted data records.

30. The system of Claim 29 wherein the SSL-based connection control circuit is further configured to establish the SSL-based protocol connection with the destination device as a pre-encrypted data records based connection.

31. A system of message authentication for an SSL-based protocol connection between a source device and a destination device, the system comprising:

a receiver that receives a first plurality of communication packets and a group MAC that was generated based on the first plurality of communication packets, wherein ones of the first plurality of communication packets do not include an associated packet MAC;

a message authentication code (MAC) generation circuit that generates a calculated MAC based on the received first plurality of communication packets; and

an error detection circuit that determines if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received group MAC.

32. The system of Claim 31 wherein:

the receiver is further configured to receive a record count, the record count indicating a number of data records to be received before a next group MAC, the next group MAC being generated based on a next plurality of communication packets corresponding the data records associated with the record count and to receive a number of data records of the next plurality of communication packets corresponding to the received record count and to receive the next group MAC;

the MAC generation circuit is further configured to generate a next calculated MAC based on the received data records of the next plurality of communication packets; and

the error detection circuit if further configured to determine if an error has occurred in the received data records of the next plurality of communication packets based on a comparison of the next calculated MAC and the received next group MAC.

33. A system of message authentication for an SSL-based protocol connection between a source device and a destination device, the system comprising:

means for generating a group message authentication code (MAC) based on a plurality of communication packets, each of the communication packets having at least one data record; and

means for transmitting the plurality of communication packets using the SSL-based protocol connection along with the generated group MAC, wherein ones of the plurality of communication packets do not include an associated packet MAC.

34. The system of Claim 33 further comprising means for transmitting a record count using the SSL-based protocol connection, the record count indicating a number of data records to be received associated with a next group MAC to be received, the data records associated with the record count corresponding to a next plurality of communication packets to be transmitted and wherein the next group MAC is generated based on the next plurality of communication packets to be transmitted.

35. The system of Claim 34 wherein the record count is transmitted using the SSL-based protocol connection before the next plurality of communication packets and wherein the next group MAC is transmitted after the next plurality of communication packets.

36. The system of Claim 33 wherein at least a subset of communication packets from the plurality of communication packets have pre-encrypted data records and wherein the system further comprises:

means for encrypting data records of the at least a subset of communication packets to provide the pre-encrypted data records;

means for storing the pre-encrypted data records;

means for retrieving ones of the stored pre-encrypted data records for transmission responsive to a request for transmission of the ones of the stored pre-encrypted data records;

means for transmitting the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection without using the SSL-based protocol connection to encrypt the retrieved ones of the stored pre-encrypted data records; and

means for transmitting a group MAC generated based on the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection to encrypt the group MAC generated based on the retrieved ones of the stored pre-encrypted data records.

37. The system of Claim 33 further comprising the destination device wherein the destination device comprises:

means for receiving the first plurality of communication packets and the generated group MAC;

means for generating a calculated MAC based on the received first plurality of communication packets; and

means for determining if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received generated group MAC.

38. A system for message authentication for an SSL-based protocol connection between a source device and a destination device, the system comprising:

means for receiving a first plurality of communication packets and a group MAC that was generated based on the first plurality of communication packets, wherein ones of the first plurality of communication packets do not include an associated packet MAC;

means for generating a calculated MAC based on the received first plurality of communication packets; and

means for determining if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received group MAC.

39. The system of Claim 38 further comprising:

means for receiving a record count, the record count indicating a number of data records to be received before a next group MAC, the next group MAC being generated based on a next plurality of communication packets corresponding the data records associated with the record count;

means for receiving a number of data records of the next plurality of communication packets corresponding to the received record count;

means for receiving the next group MAC;

means for generating a next calculated MAC based on the received data records of the next plurality of communication packets; and

means for determining if an error has occurred in the received data records of the next plurality of communication packets based on a comparison of the next calculated MAC and the received next group MAC.

40. A computer program product of message authentication for an SSL-based protocol connection between a source device and a destination device, comprising:

a computer readable storage medium having computer readable program code embodied in said medium, said computer readable program code comprising:

computer readable code which generates a group message authentication code (MAC) based on a plurality of communication packets, each of the communication packets having at least one data record; and

computer readable code which transmits the plurality of communication packets using the SSL-based protocol connection along with the generated group MAC, wherein ones of the plurality of communication packets do not include an associated packet MAC.

41. The computer program product of Claim 40 further comprising computer readable code which transmits a record count using the SSL-based protocol connection, the record count indicating a number of data records to be received associated with a next group MAC to be received, the data records associated with the record count corresponding to a next plurality of communication packets to be transmitted and wherein the next group MAC is generated based on the next plurality of communication packets to be transmitted.

42. The computer program product of Claim 41 wherein the record count is transmitted using the SSL-based protocol connection before the next plurality of communication packets and wherein the next group MAC is transmitted after the next plurality of communication packets.

43. The computer program product of Claim 40 wherein at least a subset of communication packets from the plurality of communication packets have pre-encrypted data records and wherein the computer program product further comprises:

computer readable code which encrypts data records of the at least a subset of communication packets to provide the pre-encrypted data records;

computer readable code which stores the pre-encrypted data records;

computer readable code which retrieves ones of the stored pre-encrypted data records for transmission responsive to a request for transmission of the ones of the stored pre-encrypted data records;

computer readable code which transmits the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection without using the SSL-based protocol connection to encrypt the retrieved ones of the stored pre-encrypted data records; and

computer readable code which transmits a group MAC generated based on the retrieved ones of the stored pre-encrypted data records using the SSL-based protocol connection to encrypt the group MAC generated based on the retrieved ones of the stored pre-encrypted data records.

44. The computer program product of Claim 40 further comprising the following configured for execution on the destination device:

computer readable code which receives the first plurality of communication packets and the generated group MAC;

computer readable code which generates a calculated MAC based on the received first plurality of communication packets; and

computer readable code which determines if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received generated group MAC.

45. A computer program product of message authentication for an SSL-based protocol connection between a source device and a destination device, comprising:

a computer readable storage medium having computer readable program code embodied in said medium, said computer readable program code comprising:

computer readable code which receives a first plurality of communication packets and a group MAC that was generated based on the first plurality of communication packets, wherein ones of the first plurality of communication packets do not include an associated packet MAC;

computer readable code which generates a calculated MAC based on the received first plurality of communication packets; and

computer readable code which determines if an error has occurred in the received first plurality of communication packets based on a comparison of the calculated MAC and the received group MAC.

46. The computer program product of Claim 45 further comprising:

computer readable code which receives a record count, the record count indicating a number of data records to be received before a next group MAC, the next group MAC being generated based on a next plurality of communication packets corresponding the data records associated with the record count;

computer readable code which receives a number of data records of the next plurality of communication packets corresponding to the received record count;

computer readable code which receives the next group MAC;

computer readable code which generates a next calculated MAC based on the received data records of the next plurality of communication packets; and

computer readable code which determines if an error has occurred in the received data records of the next plurality of communication packets based on a comparison of the next calculated MAC and the received next group MAC.